REMARKS

Claims 68-87, 95, 97-100, 102, and 103 are pending and stand rejected. The applicant respectfully requests reconsideration and allowance of the pending claims in light of the following.

I. Claim Rejections Under 35 U.S.C. § 103 (Alcorn, Davis, and Ohno)

The Office Action rejected claim 68-87, 95, 97-100, 102, and 103 under U.S.C. § 103(a) as being unpatentable over US 5,643,086 to Alcorn et al., hereinafter "Alcorn," in view of US 5,539,828 to Davis, hereinafter "Davis, " and US 5,355,413 to Ohno, hereinafter "Ohno." The applicant respectfully requests reconsideration in light of the following.

A. Claims 68-74

Each of claims 68-74 is directed to a system comprising, among other things, an authorization agent apparatus configured to "transmit an authentication algorithm to said gaming machine, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to authenticate said gaming software; [and] receive from said gaming machine an outcome of said authentication algorithm applied to said gaming software." The applicant respectfully submits that the proposed

combination of Alcorn, Davis, and Ohno does not teach or otherwise render obvious such aspects of claims 68-74.

The applicant respectfully submits that the Office Action appears to misunderstand and/or mischaracterize the operation of the Alcorn device in regard to remotely demanding authentication. The applicant believes such misunderstand/mischaracterization may have resulted in the belief that the Alcorn device is closer in operation to the claimed invention, than the Alcorn device is in fact.

For example on page 13, the Office Action contends in regard to Alcorn:

> The authentication can be conducted locally or externally via a network (4:39-58). This external authentication is used to authenticate ROM 29 in the same manner as ROM 29 authenticates the mass storage unit and the rest of the contents of the gaming machine (8:38-52); in this case the authentication program would necessarily be external to the gaming machine. This can be done for example, by the gaming commission (8:54-62), so the gaming machine would receive a verification algorithm from the external source and send it back to the external authentication agent (9:47-58).

The applicant respectfully disagrees with such assessment of Alcorn. In regarding to such network operation, Alcorn merely teaches sending a demand via a network to the gaming machine to cause the gaming machine to initiate its authentication procedure. It's fairly clearly, when taken in context, such network demand is merely one of many described manners of triggering the authentication

procedure, which is executed locally by the gaming machine. For example, Alcorn indicates that the gaming machine may execute the authentication procedure: (i) each time the game is loaded from the mass storage unit into main memory 13; (ii) in response to the pull of a slot game handle; (iii) in response to the detection of a coin inserted into the gaming machine; (iv) in response to the payout of coins or the issuing of credit; (v) in response to activating a manually operated switch on the gaming machine that is only accessible to authorized persons; and (vi) in response to a demand command generated remotely and transmitted to the gaming machine over a network. See, Alcorn 9:27-57.

At 8:1-26, Alcorn explains the execution of its authentication routine. As is clear from 8:1-26, the authentication routine is executed locally by the gaming machine using only locally stored routines. Furthermore, Alcorn clearly indicates that in order to prevent tampering such routines must be stored in an unalterable ROM 29. See, Alcorn 7:12-14 and 8:26-67. As such, Alcorn provides a clear teaching away from the proposed modification of having an external device provide the authentication routine via the network. Such a modification would thwart Alcorn's protections against unauthorized change and/or bypassing of the authentication routine, namely, the storing of such routines in unalterable ROM 29.

Moreover, despite the Office Actions contentions on page 14 to the contrary, Alcorn never mentions or otherwise suggests receiving a verification algorithm from an external source (e.g., a gaming commission) and sending the verification algorithm back to the external authentication agent. The applicant appreciates that Alcorn in various paragraphs mentions that an external agent, such as a gaming commission, may authenticate the gaming machine. However, the applicant has found no mention or suggestion in Alcorn that such authentication involves the transfer of an authentication routine from the gaming commission over a network to the gaming machine for execution by the gaming machine in the manner suggested by the Office Action.

In fact, Alcorn at 3:22-33 clearly indicates that authentication of the Alcorn device is conducted in the same way as that now performed in prior art devices: viz. computing the message digest directly from the unalterable read only memory device, and comparing the message digest with the custodial version. It should be appreciated that such a comparison merely requires the custodian (e.g., gaming commission) to maintain a custodial copy of the contents of the read only memory device, compute a message digest from the contents, and compare such message digest to a message digest computed by the gaming machine. Such a process does not require the transfer of authentication routines from the gaming commission to the gaming machine for

execution by the gaming machine as the Office Action appears to contend. See, Office Action at page 14.

Moreover, the remote triggering of the authentication routine from the gaming commission via the network is presumably done to cause the gaming machine to compute the message digest and send the digest to the gaming commission via the network. However, the applicant points out that Alcorn does not appear to explicitly disclose the sending of the digest to the gaming commission via the network. Instead, Alcorn appears to only describe the triggering of the authentication procedure via the network. The actual transfer of the message digest to the gaming commission may occur via different means as such aspect is simply not disclosed.

The applicant respectfully submits that Davis adds very little to the teachings of Alcorn in regard to above discussed aspects of claims 68-74. As noted above, Alcorn teaches that the authentication procedure may be triggered remotely by sending a command over the network. Davis basically teaches the same technique. In particular, a remote agent generates a challenge which results in the device to be verified generating a response. If the response is as expected, the remote agent has verified the device's identity and the remote agent may continue encrypted communications with the device. Otherwise, the remote agent determines that the device's identity can not be verified, and the remote agent discontinues communications with the device. Similar to

Alcorn, the remote device in Davis does not send an authentication routine to the device for execution. Instead, the remote device in Davis sends the device to be verified a random challenge and determines whether the appropriate response is received. See, Davis 6:39-7-24.

In order to further address this shortcoming of Alcorn and Davis, the Office Action further cites Ohno. In particular, the Office Action on page 5 contends that Ohno teaches an authentication algorithm transmitted from one device to another. The applicant respectfully disagrees. Ohno does not teach transferring an authentication algorithm from one device to another, but instead teaches transferring encryption algorithms (f'1)(g'2) to IC card 13. The applicant respectfully points out that such encryption algorithms are merely a portion of a larger authentication procedure executed by the IC card 13 and is not the authentication procedure itself. The embodiment relied upon by the Office Action corresponds to Fig. 15 in which step 145 is the authentication process. However, as noted at 8:40-42, the authentication process is the same authentication operation as that executed in previous embodiments. One such embodiment is depicted in Fig. 4 and another such embodiment is depicted in Fig. 5. Based upon Figs. 4 and 5, its clear that encryption algorithms (f'1)(g'2) are not authentication algorithms as contended, but merely encryption algorithms used by an authentication process.

Furthermore, the applicant points out that Ohno merely authenticates the IC card based upon whether the IC card has an expected authentication code stored in the IC card. The authentication operations shown in Figs. 4 and 5 are not applied to software of the IC card to authenticate such software, let alone, applied to gaming software of the IC card to authenticate such gaming software as required by claims 68-74. Accordingly, Alcorn, Davis, and Ohno in combination fail to teach or otherwise render obvious transferring an authentication algorithm to the gaming machine to be (i) executed by the gaming machine and (ii) applied to gaming software of the gaming machine. Moreover, the applicant further submits that Alcorn teaches away from such a modification of the Alcorn device as Alcorn clearly states that the authentication procedures **must** be stored the unalterable ROM 29 in order to prevent tampering. Such aspects of Alcorn clearly teach away from modifying the Alcorn device in a manner that results in the Alcorn device receiving such authentication procedures via a network as proposed.

In light of the above, the applicant respectfully requests the present rejection of claims 68-74 be withdrawn.

B. Claims 75-78

Each of claims 75-78 is directed to a method that comprises, among other things, "transmitting an authentication algorithm from said external authentication agent

apparatus to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine." The applicant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 75-78. Accordingly, the applicant respectfully requests withdrawal of the present rejection of claims 75-78 for reasons similar to those presented above in regard to claims 68-74.

C. Claim 79

Claim 79 is directed to a gamine machine comprising, among other things, "a process to … process an authentication algorithm received via the interface, and wherein the authentication algorithm comprises a plurality of instructions to be executed by the processor of said gaming machine to authenticate said data files of games." The applicant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claim 79. Accordingly, the applicant respectfully requests withdrawal of the present rejection of claims 79 for reasons similar to those presented above in regard to claims 68-74.

D. Claims 80-87

Each of claims 80-87 is directed to a method that comprises, among other things, "transmitting via a communication link an authentication algorithm to said gaming machine from an authentication agent apparatus, the authentication algorithm

including at least one instruction arranged for processing by said gaming machine to derive an outcome of said one or more program files." Again, the applicant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 80-87. Accordingly, the applicant respectfully requests withdrawal of the present rejection of claims 80-87 for reasons similar to those presented above in regard to claims 68-74.

E. Claims 95, 97-100, 102, and 103

Each of claims 95, 97-100, 102, and 103 is directed to a system that comprises, among other things, "an authentication agent apparatus … configured to: transmit an authentication algorithm to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine to derive an outcome of said authentication algorithm applied to at least said portion of said gaming machine." Again, the applicant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 95, 97-100, 102, and 103. Accordingly, the applicant respectfully requests withdrawal of the present rejection of claims 95, 97-100, 102, and 103 for reasons similar to those presented above in regard to claims 68-74.

II. Final Matters

The Office Action makes various statements regarding: the pending claims; the Alcorn, Davis, and Ohno references; 35 U.S.C. § 103; and the state of the art that are now moot in view of the previously presented amendments and/or remarks. Thus, the applicant has not addressed all of such statements at the present time. However, the applicant expressly reserves the right to challenge any of such statements in the future should the need arise.

CONCLUSION

The applicant submits that the pending claims are in condition for allowance. The applicant thus requests an expeditious notice of allowability with respect to all pending claims. If the examiner disagrees, the applicant requests an Examiner Interview to discuss the pending claims and the restriction/election requirement. The applicant invites the examiner to contact the undersigned at 312-238-8600 to arrange such an interview.

The Commissioner is hereby authorized to charge additional fees or credit overpayments to the deposit account of McAndrews, Held & Malloy, Account No. 13-0017.

Date: May 9, 2011

Respectfully submitted,

/Jeffrey B. Huter/
Jeffrey B. Huter
Reg. No. 41,086
Attorney for the Applicants

McANDREWS, HELD & MALLOY, LTD.
500 W. Madison, Suite 3400
Chicago, IL 60661
Telephone: (312) 775-8000
Direct: (312) 238-8600